

Strengthening DoD's Identity Assurance Through an Enterprise-Wide Biometrics Solution

Biometrics—A Prime Security Enabler that Cannot be Lost, Forgotten, Forged, or Stolen

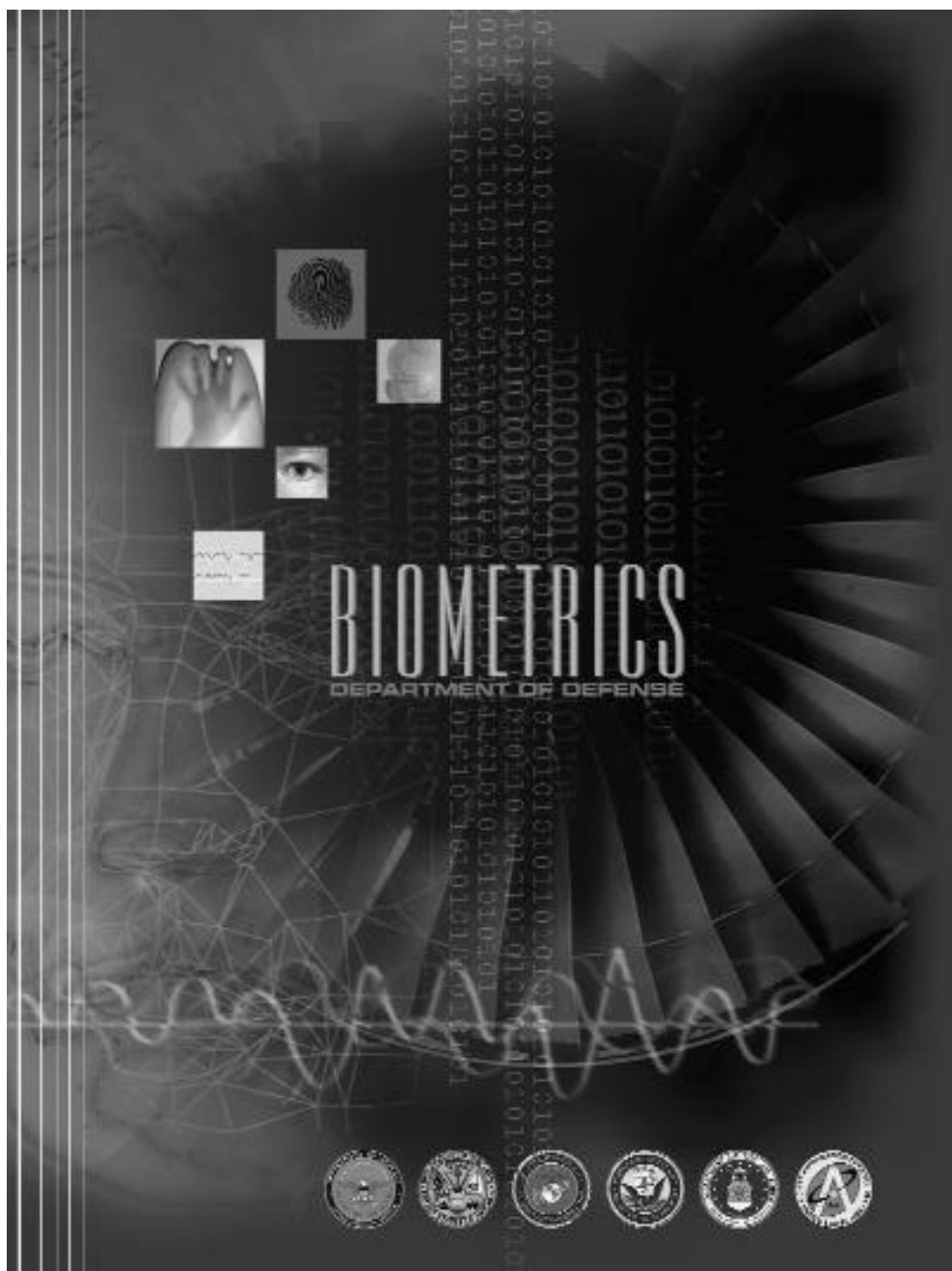
DR. LINDA DEAN • MAJ. STEPHEN FERRELL, USA • LYDIA KAIZER

Imagine what it might be like for DoD employees, even when transferring from one area to another, to be able to easily access their computers and workplaces with the touch of a finger to a platen device, or by glancing into an iris scanner. Imagine, more importantly, what it might be like for the DoD to know that users are able to access only the facilities and information to which they have been granted authority.

Traditional Forms of Identification Fall Short

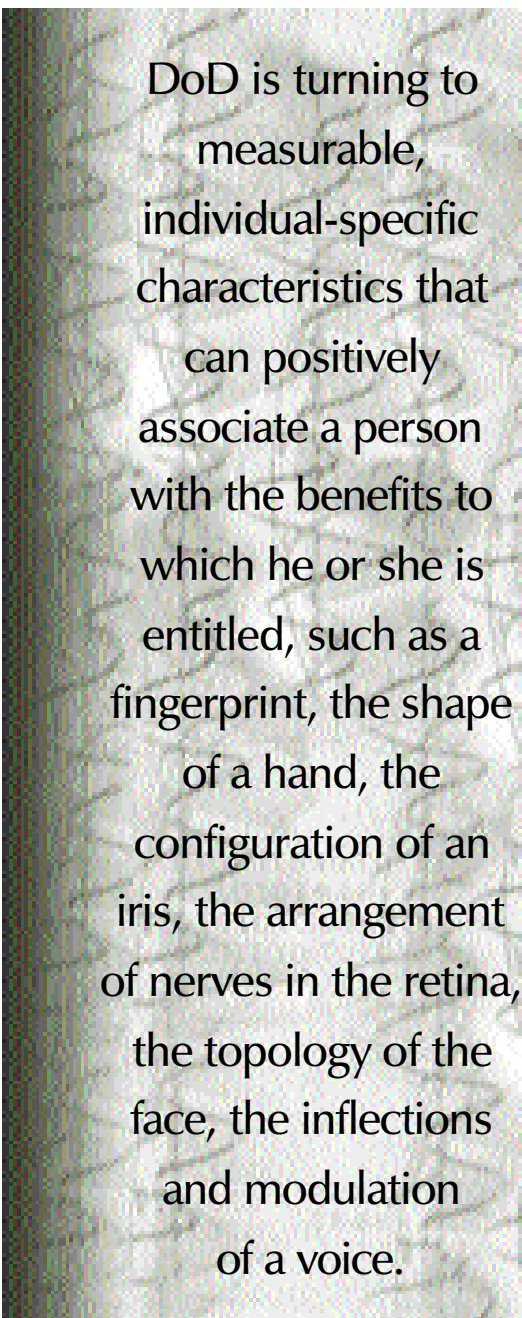
The challenge to achieving such an end-state is easily stated: how does the DoD guarantee—at any given time, in any given location—that a person claiming authority to access valuable internal assets is actually the person to whom such authority has been granted? Recent events have made it clear that something in addition to the traditional forms of identification—photo IDs, Personal Identification Numbers (PINs) and passwords—might be necessary to meet this challenge. A tool is needed that cannot be lost or forgotten, forged or stolen; that can guarantee the identity, or verify the claimed identity, of an individual; that can ensure that the right person with the right privileges has timely access to secure systems and facilities

Dean is Director of the DoD Biometrics Management Office (BMO), located in Arlington, Va. Her full bio appears on p. 5 of this article. *Ferrell* is Director, Biometrics Fusion Center, BMO; and *Kaizer* is with Booz, Allen & Hamilton, providing policy contract support to the BMO.



across the DoD enterprise; and that can positively link an individual with certain activities or events.

To achieve these levels of identity assurance, the DoD is turning to measurable, individual-specific characteristics that can positively associate a person with the benefits—including facility and network access—to which he or she is entitled. These characteristics are referred to as biometrics. They include certain physical patterns and geometries that are unique to each human being: a fingerprint, the shape of a hand, the con-



DoD is turning to measurable, individual-specific characteristics that can positively associate a person with the benefits to which he or she is entitled, such as a fingerprint, the shape of a hand, the configuration of an iris, the arrangement of nerves in the retina, the topology of the face, the inflections and modulation of a voice.

figuration of an iris, the arrangement of nerves in the retina, the topology of the face, the inflections and modulation of a voice.

Each of these and other individual-specific identifiers can be captured, measured, converted to a mathematical algorithm, and recorded for future use. Moreover, because they represent who you are, instead of what you know (a PIN or password) or what you possess (a token or key), each has the potential to allow for guaranteed identity assurance. That, in turn, translates to guaranteed security of the DoD's physical and information assets.

The DoD is no stranger to biometric technologies; the Department has been using these technologies to manage access to chemical demilitarization projects for many years. More recently, the Department has begun using iris scan and fingerprint technologies to manage physical access to restricted properties and logical access to critical computers and networks.

Looking to the future, the DoD is investing heavily in the research, development, and evaluation of emerging biometric technologies, including facial recognition, hand geometry, signature verification, and voice recognition, to determine their operational viability. A list of qualified devices, however, is only half the equation. The question remains: how do you make each device functional within an enterprise as massive, multifaceted and geographically dispersed as the DoD?

The DoD Biometrics Management Office

In 2000, the United States Congress directed the Secretary of the Army to act as Executive Agent in leading, consolidating, and coordinating all biometrics information assurance programs for the DoD. To accomplish this mission, the Army created a DoD Biometrics Management Office (BMO). The mission of the BMO is to ensure that biometrics technologies are integrated effectively into information assurance programs, physical access control systems, and best

business practices across the DoD. This mission entails two clearly defined objectives: 1) to test and evaluate currently available biometrics products for DoD applications; and 2) to develop an enterprise solution to facilitate the use of biometrics across the DoD.

Device Testing

The BMO maintains two criteria for selecting the biometric devices that it evaluates.

COTS Product

First, the device must be a Commercial-Off-the-Shelf (COTS) product. Through close working relationships with research and development organizations such as the Defense Advanced Research Projects Agency (DARPA), the BMO keeps informed of cutting-edge technology developments in the biometrics arena. Its mandate, however, is to build a solution that will satisfy current DoD requirements.

Interoperability

Second, the BMO considers only those devices that have the potential to integrate into a large, enterprise-wide solution. Interoperability is critical. Once these prerequisites are satisfied, the Biometrics Fusion Center (BFC), located in West Virginia, steps in to perform comprehensive testing.

There are three phases to the BFC's product testing process.

Product Assessment Phase

All devices claim certain levels of technical performance. The BFC's Product Assessment phase determines to what degree those claims are valid, and whether or not they meet certain DoD-determined minimum performance standards.

Controlled Environment Testing

The second phase of the evaluation process, Controlled Environment Testing, introduces each device to a set of conditions intended to determine if an item—in addition to being technically viable—can remain technically viable in various DoD operational environments. Devices are subjected to extremes

of illumination, temperature, humidity, physical stress, operational repetition, particulate contamination, and electronic and magnetic interference. The data collected from these evaluations allow the BFC to match device capabilities with specific DoD operational requirements.

Field Testing

Those devices that meet one or more DoD operational requirements are graduated to the final phase of the evaluation process. Field Testing involves physical deployment of selected devices to the operational environments in which they will have to function. Their performance during this phase will establish the military applications for which they will be appropriate, and the level of security that they will be able to provide within each application.

The result of these testing activities will be a DoD Biometrics Product List. This is the list from which DoD executives and commanders will select biometric devices that meet their specific identity assurance requirements.

Enterprise Solution Development

The BMO plans to reach Full Operational Capability (FOC) of its biometrics enterprise solution by the second quarter of fiscal 2005. The devices, systems, network architecture, and business processes that comprise this solution will allow for worldwide deployment of biometric identification devices to safeguard access to DoD facilities and information.

The goal of this development initiative is summarized in a phrase coined early on by the BMO: *one enrollment, multiple uses*. The idea is to provide the DoD with the ability to: 1) rapidly, accurately, and securely authenticate personal identity based upon one or more of an individual's biometric characteristics; and 2) to exchange that individual's biometric credentials between authorized entities in a secure and trustworthy fashion.

Once fully operational, the DoD's biometrics solution may be used as a standalone access security tool or—especially

in those instances when the facility or network in question is of particular importance—it may become part of a layered solution, serving in concert with other, more traditional forms of identification.

The DoD Biometrics Senior Coordinating Group

To ensure that the security requirements of the various Agencies, Departments, and Services within the DoD are adequately represented as the BMO proceeds with evaluating biometric devices and with building a biometrics enterprise solution, the Army, acting as executive agent, also has formed a DoD Biometrics Senior Coordinating Group (BSCG). Similar in function to a board of directors, this group is composed of senior military and civilian executives across the DoD.

Its mission is to provide strategic guidance to the DoD BMO on the development, evaluation, and implementation of biometrics enterprise solutions; and to serve as the DoD-wide coordinating group for biometrics issues. This mission entails, among other things, the development and implementation of policy, and the promotion of selected technical and business process standards.

Policy

In order for the DoD to successfully deploy a biometrics enterprise solution, policy must be created and implemented to allow for and manage the use of this solution. The BSCG endorses and provides advocacy for policy governing the collection, storage, retrieval, and use of biometric data within DoD. This provides the needed horsepower to implement those plans, and provides the DoD biometrics end-users with the guidance they need to best employ these new technologies for security or business process improvement.

Standards

As information and resource sharing becomes an ever-increasing priority across all government departments, the BSCG recommends and promotes the use of federal, national, and international stan-

dards or common commercial practices for biometrics. This maximizes interoperability between biometrics applications, helping the biometrics industry meet DoD technology requirements in an efficient manner. By reducing the adoption of technologies that cannot interact with other systems of similar purpose but different architectures, this interaction between industry and government is a benefit to taxpayers as well.

Building the Component Pieces

The BMO has identified four stages in the life of a biometric:

- Collection
- Storage
- Access and Retrieval
- Use

Each of these stages, or functional areas, poses a unique set of requirements that must be satisfied individually, but must also work within the larger context of an integrated solution. For each functional area, there are five phases to the development process:

- Design
- Build
- Test
- Field
- Integrate

The final phase, integration, involves the incorporation of the solutions developed within each functional area (Collection, Storage, Access and Retrieval, and Use) into a unified architectural whole. To create best-of-breed solution sets for each area, the BMO has created four Enterprise Working Groups (EWGs) to identify requirements and design and implement Technology Demonstrations (TDs).

The Collection Enterprise Working Group

This EWG is responsible for researching and recommending the best biometrics collection system configurations to become part of the enterprise solution's operational, systems, and standards architectures. To ensure scalability, this group will focus primarily on

DR. LINDA S. DEAN

DoD BIOMETRICS MANAGEMENT OFFICE

*Office of the Secretary of the Army
Corporate Information Office/G6*

Dr. Linda S. Dean became the Director, DoD Biometrics Management Office on Aug. 1, 2002. As the Director, Dean is currently overseeing the development of DoD biometric policies and enterprise solutions for physical and logical access uses crossing all functional areas including finance, logistics, personnel, acquisition, information management, and medical.



Program (CEAP), and the Army's Super Computer Program.

Dean served as Chief of the Resource Management Division, Software Development Center, Fort Lee, Va., and as Chief of the Program and Budget Division, Headquarters, Information Systems Engineering Command, Fort Belvoir, Va. (1984-1987). In both positions

she centrally managed Army-wide annual operating budgets amounting to \$60 million and \$756 million respectively.

While serving as a comptroller careerist, she held journeyman program analyst positions in both the Army's Training and Doctrine Command and the Information Systems Command (1981-1984). She entered the Army's Comptroller career field as an Army Materiel Command Intern at Corpus Christi Army Depot in August 1979. Prior to the internship, she spent six years (1973-1978) working in both supervisory and non-supervisory positions in Army finance and accounting offices at Fort Monroe, Va.; Fort Jackson, S.C.; and the Army Corps of Engineers Middle East Division (Rear) in Berryville, Va.

Dean earned her Doctorate in Public Administration from the University of Southern California, Washington Public Affairs Center, Washington, D.C. She holds a Masters of Public Administration from the University of Southern California, Washington Public Affairs Center, Washington, D.C., and a Bachelor of Arts (with honors) in Human Resource Management from Saint Leo's College, Fla.

Dean's executive training includes the Professional Military Comptrollership Program at the Air University, Maxwell Air Force Base, Ala., in 1983 (her team received the academic achievement award); the U.S. Army Mid-Career Executives Program in Public Administration during 1986 through 1987; and, the Federal Executive Institute Program for Leadership in a Democratic Society in 1995.

Prior to assignment in this position, from October 1999 to August 2002, Dean served as the Army's Corporate Information Office's (CIO) C4 Enabling Technologies Director where she directed the implementation of the Army's Common Access Card and Public Key Infrastructure programs, which provide a standardized DoD smart card technology solution for personal identification, digital signatures, and email encryption.

From October 1997 to August 1999 she served in the Army's Office of the Director of Information Systems for Command, Control, Communications, and Computers (DISC4) as the Director, Electronic Commerce (October 1990 through September 1997) and Director, C4 Policy (October 1997 through September 1999), respectively. While in those policy positions, she managed the development of Army-wide policy direction contained in over 200 regulations, pamphlets, and Army policy letters, for the Army's five information mission area disciplines, which included: automation; telecommunications; printing and publishing; visual information; and records management.

Before joining the ODISC4 staff, from 1987-1990, she served as a senior program analyst in the Army's Program Executive Office, Standard Army Management Information Systems (PEO STAMIS). As a senior analyst, she was responsible for oversight of program management activities for several high-dollar (greater than \$100 million in life cycle costs) Army Information Systems, including the Army's Computer Aided Logistics System (ACALS), the Corps of Engineers Automation

the most widely used biometrics technologies, such as fingerprint and iris scan, to serve as a program baseline. Dependence on other biometric technologies, such as voice and facial recognition, will grow as those systems become more mature and are able to satisfy user requirements. The intent is to identify biometric collection devices that will meet user requirements regardless of location or environment, including devices used for both physical and information access.

One solution currently under review by the Collection EWG is to leverage all or portions of the DoD's existing personnel information collection infrastructure. These include:

- All 65 United States Military Entrance Processing Command Stations.
- All fixed Real-time Automated Personnel Identification System locations (RAPIDS).
- All portable RAPIDS workstations that issue Common Access Cards (CACs) within the DoD.

In any event, candidate collection solutions are scheduled for testing during the TD phase in the fourth quarter of fiscal 2003.

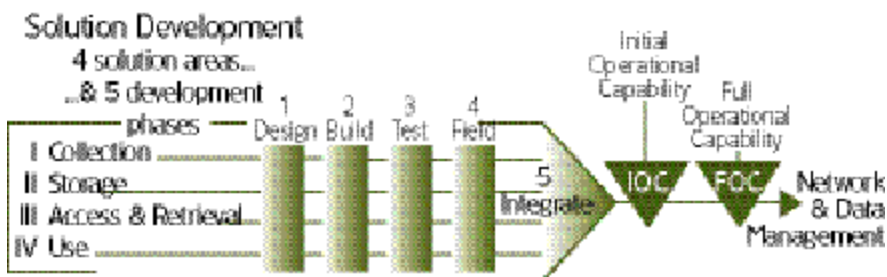
The Repository Enterprise Working Group

This EWG is tasked with identifying the most relevant biometric storage solutions to enhance DoD business and tactical functions. To achieve this goal, the group is focused on researching and recommending optimal biometric repository configurations for local, regional, and central repositories. Candidate repository solutions for local and regional repositories are scheduled for testing in the fourth quarter of fiscal 2003.

Access and Retrieval Enterprise Working Group

The next step in the process is to identify the communications architecture that will best support secure access, retrieval, and management of biometrics data. Working closely with the Defense Manpower Data Center (DMDC), the Access and Retrieval Enterprise Work-

FIGURE 1. DoD Biometrics Management Office Enterprise Solution Development



ing Group is tasked with guiding the design and development of this optimal architecture.

As with the processes previously described, candidate solutions identified by the Access and Retrieval EWG will be tested in the fourth quarter of fiscal 2003.

Use Enterprise Working Group

The Use Enterprise Working Group is responsible for carefully considering DoD end-user requirements in designing an enterprise solution. This group is working closely with the RAND Corporation, which has been tasked with surveying multiple DoD organizations to identify user requirements. Consolidated user feedback is expected during the second quarter of fiscal 2003, in time for candidate solution testing in the fourth quarter of fiscal 2003.

In addition to the four EWGs that constitute the core of the BMO's enterprise solutions development program, five specialized working groups are charged with addressing program-wide enterprise architecture, requirements, policy, legal, and economic issues.

- The **Enterprise Architecture** working group is tasked with determining the optimal architectural configuration between DoD users and the central repository.
- The **Requirements** working group is responsible for identifying functional requirements from the Uniformed Services, DoD civilian political leadership, the Joint Staff, and other DoD agencies to establish future regulations.

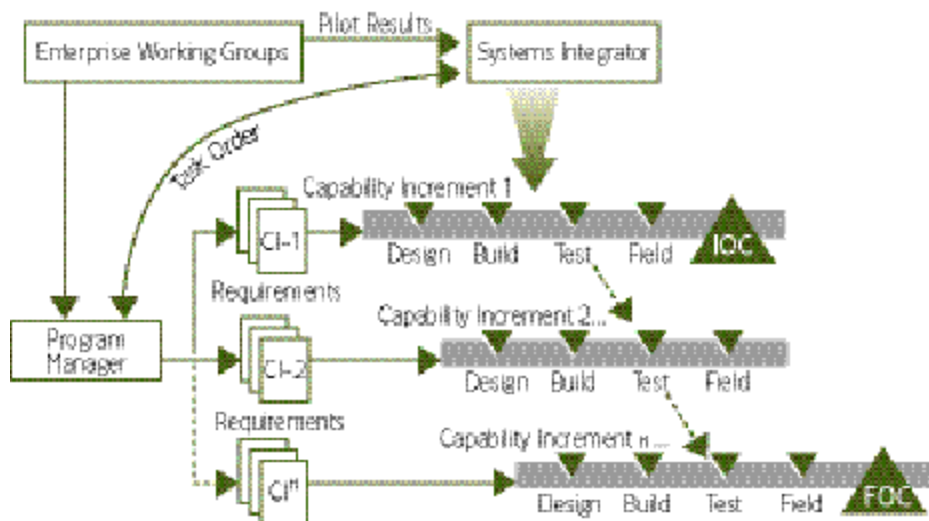
- The **Policy** working group is charged with developing a prescriptive, incremental DoD policy framework that mandates policies and procedures for how biometrics will be acquired, stored, and used.
- The **Legal** working group is tasked with establishing regulatory authority and guidelines for proper collection and disposal of biometrics from active and reserve military personnel, civilians, contractors, family members, and foreign personnel hired by the DoD.
- Finally, the **Functional Economic Analysis** working group is responsible for defining alternatives to support the Program Objective Memorandum (POM) process, and for delivering a cost-benefit model to validate the implementation of the enterprise solution.

Putting the Pieces Together

Once the TDs are complete, the BMO will integrate these functional solutions into a comprehensive Enterprise Architecture. Parallel to this effort, the BMO will develop a policy framework to establish procedures for the collection, storage, and use of biometrics within DoD. Leveraging both the technology solutions and the policy framework, the BMO plans to reach Initial Operational Capability (IOC) by the second quarter of fiscal 2004 and FOC by the second quarter of fiscal 2005. Figure 1 to the left illustrates this process.

During the IOC phase, the BMO will introduce its integrated enterprise solution on a smaller scale to various test populations. This important phase will allow the BMO to identify user concerns regarding technology and operational components of the solution. This information will provide the BMO with a clear picture of which best-of-breed biometric technologies are best suited within each environment, and will allow for fine-tuning and adjusting of the solution as a whole. Collected over the 12-month duration of the IOC phase, this information will drive the Biometrics Management Office's migration plans, as well as its acquisition and deployment plans, for scaling and implementing the solution to FOC across the DoD.

FIGURE 2. DoD Biometrics Management Office Enterprise Solution Management



Enterprise Solution Management

Once the enterprise solution has achieved FOC, the focus of the DoD's biometrics program turns to maintaining and securing DoD biometric data and managing the network over which those data are exchanged. However, the rapidly evolving nature of biometric technologies will continue to present challenges and opportunities for improvement. In fact, as illustrated in Figure 2 on the preceding page, the development of a biometrics enterprise solution is itself an ongoing, iterative process.

This approach follows a "build as you grow" concept, dividing the system into several useful, supportable, and operational increments. In growing biometrics capability, demonstrated technology and operational concepts are incorporated into sequential Capability Increments (CIs). As each CI completes the build phase, it becomes the baseline for the next increment. This ongoing process will ensure that the BMO continues to meet its mission within the DoD, and will ensure that the DoD possesses the identity assurance system that it needs to meet its mission to the people of the United States.

Biometrics—A Prime Security Enabler

As the DoD moves further into the digital age, biometrics serve as a prime security enabler by ensuring positive identification of those accessing critical systems and facilities. This technology offers countless uses for military applications in future systems, including information assurance, force protection, and access control. However, mature technology adoption takes a deliberate, conservative approach in order to achieve optimal effectiveness. The DoD's initiative with the BMO's biometric Enterprise Solution assumes this course of action to ensure that the resulting system architecture is interoperable, scalable, and able to meet the growing demands of our transforming military.

Editor's Note: The authors welcome questions or comments on this article. Contact ssadlon@brtrc.com.

Defense Acquisition University Awarded National Accreditation

FORT BELVOIR, Va. (Feb. 4, 2003)—The Commission of the Council on Occupational Education (COE) has granted accreditation to the Defense Acquisition University, located at Fort Belvoir, Va. Announcement of the action was made by Harry L. Bowman, Executive Director, Commission of the Council on Occupational Education (COE), following the Commission's meeting held in Atlanta, Ga., Feb. 2-4, 2003.

The award of accreditation status is based on an evaluation to demonstrate that the institution meets not only the standards of quality of the Commission, but also the needs of students, the community, and employers.

The Commission's evaluation process includes an extensive self-study by the institution and an intensive review by a visiting team of professional educators representing the Commission's member institutions from other states.

The Defense Acquisition University began its self study in July 2000 and underwent a team visit in November 2002. The visiting team chairperson was James Conely.

The COE, based in Atlanta, Ga., offers quality assurance services to post-secondary workforce education providers across the nation. Organized as a non-profit corporation, the mission of the Council is to assure quality and integrity in career and workforce development. Services offered include institutional accreditation (recognized by the U.S. Department of Education), program quality reviews for states and workforce education providers, and informational services. Most of the Council's work is carried out by qualified professional volunteers who are experts in workforce education.

Institutional membership in the Council is voluntary, but can be achieved only by becoming accredited. The Council's current membership makes it unique. Members include postsecondary public technical institutes, specialized military and national defense schools, Job Corps Centers, private career schools, non-profit workforce education providers, corporate and industry education units, and federal agency institutions. No other agency accredits and serves the diversity of organizations served by the Council. There are approximately 410 institutional members at the present time.

The Defense Acquisition University, with headquarters at Fort Belvoir, Va., has regional campuses in Patuxent River, Md.; Dayton, Ohio; Huntsville, Ala.; and San Diego, Calif. For its primary mission, DAU provides training and education to approximately 129,000 practitioners in the Department of Defense Acquisition, Technology and Logistics Workforce (DoD AT&L).

Editor's Note: To view the DAU 2003 Course Catalog, visit <http://www.dau.mil> and click on "DAU Courses."

